

**IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

SECURITIES AND EXCHANGE)	
COMMISSION,)	
)	
Plaintiff,)	
)	Civil Action No. 1:23-cv-09518-PAE
v.)	
)	
SOLARWINDS CORP. and TIMOTHY G.)	
BROWN,)	
)	
Defendants.)	

DEFENDANTS’ STATEMENT OF UNDISPUTED MATERIAL FACTS¹

Defendants wish to be clear: All of the material facts needed to decide this case are contained in paragraphs 1-157 of the parties’ joint statement of undisputed facts. ECF No. 166. Based on those facts alone, summary judgment for Defendants is warranted.

Defendants file this separate Statement of Undisputed Material Facts only because the SEC has indicated that it intends to rely on the documents described below in opposing summary judgment.² Defendants deny that any of these documents are material, but, in anticipation of the SEC’s reliance on them, Defendants set forth below undisputed facts concerning these documents. These facts are “material” only insofar as they show that the documents cited by the SEC are immaterial and that the inferences the SEC seeks to draw from them are unreasonable.

¹ Citations to “JS __” refer to the parties’ Joint Statement of Undisputed Facts (ECF No. 166); Citations to “Ex. __” refer to the exhibits attached to the concurrently filed Declaration of Serrin Turner in Support of Defendants’ Motion for Summary Judgment. Citations to “[Last Name] Decl.” refer to the concurrently filed declarations of Rani Johnson, Steven Colquitt, Danielle Campbell, Róbert Krajčír, Lee Zimmerman, Tim Brown, and Gregory Rattray.

² See JS ¶¶ 157-200 (describing various documents the SEC considers relevant to certain representations in the Security Statement).

Table of Contents

I.	Document the SEC Relies on as to the NIST Cybersecurity Framework Representation.....	1
II.	Documents the SEC Relies on as to the Role-Based Access Controls Representation.....	2
A.	June 2017 Slide Proposing More Granular Controls for Administrators’ Accounts	2
B.	Documents about Efforts to Centralize and Automate Access Provisioning	4
1.	January 2018 Slide about Evaluation of Access Management Tools	4
2.	September 2018 Slide about Limited Access Management Tooling.....	6
3.	August 2019 NIST Scorecard about Pending Migration to Azure AD and Related Notations in Later QRR Presentations	7
C.	March 2020 Slide about User Access Review for SOX Audit	9
D.	“Preliminary Review” Relating to FedRAMP Certification.....	10
E.	Engineer’s Concerns about Employees Using Personal Laptops on VPN	16
F.	August 2017 Budget Request and October 2018 Draft Update.....	16
III.	Documents the SEC Relies on as to the Password Representation	19
A.	March 2018 Slide about Progress on User Account Audit.....	19
B.	November 2019 Email Chain about Developer Access to Billing Data for Test Purposes	22
C.	November 2019 Discovery and Remediation of “solarwinds123” Password	23
D.	Control Deficiencies found in FY 2019 SOX Audit.....	25
IV.	Documents the SEC Relies on as to the Secure Development Lifecycle Representation.....	26
A.	January 2018 Email about “Feedback” on Secure Software Development.....	26
B.	February 2019 Slide about Goals for MSP Engineering	31
C.	Documents about Penetration Testing	32
1.	Budget Item for External Penetration Testing in November 2018 Slide Deck.....	32
2.	July 2020 Slide about Testing in Final Security Reviews	33
D.	Documents about Threat Modeling	35
1.	May 2018 Email about Tool for Threat Modeling.....	35
2.	July 2019 MSP Products Evaluations	37
E.	June 2020 Email about Orion Improvement Program	38

I. DOCUMENT THE SEC RELIES ON AS TO THE NIST CYBERSECURITY FRAMEWORK REPRESENTATION

1. The only document the SEC cites as relevant to the NIST Cybersecurity Framework is a draft of a “policy documentation audit” emailed to Tim Brown on April 19, 2021 (after the Relevant Period), from which the SEC cites language stating that “about 40% of the baseline controls within NIST [800-53] were met or partially met.”³

2. This referenced audit reviewed the extent to which the Company had *policy documentation* in place corresponding to the controls in NIST Special Publication 800-53 (“NIST 800-53”). It was not an audit of whether the Company had implemented NIST 800-53 controls in practice.⁴

3. This was specifically labeled a draft document and was based only on policy documentation currently in SolarWinds’ policy library and policy guidance already published by Human Resources and Legal.⁵

4. After receiving this draft, Tim Brown asked the person who prepared it how the results would change if it included policies that were currently being drafted or under review. The drafter responded that “we could probably get up to 80% compliance.”⁶

5. In any event, NIST 800-53 is distinct from the NIST Cybersecurity Framework (“NIST CSF”) referenced in the Security Statement.⁷

³ JS ¶ 157; Ex. 41 (SW-SEC00185450) at -451.

⁴ Ex. 41 (SW-SEC00185450) at -451 (referencing the document as a “policy and procedures documentation audit”); *id.* (explaining that objective was to prepare policies for “annual policy reviews” and that scope of review only encompassed “policy documentation”).

⁵ Ex. 41 (SW-SEC00185450) at -451.

⁶ Ex. 42 (SW-SEC-SDNY_00046821) at -821.

⁷ JS ¶ 63; Ex. 50 (Graff Dep.) 106:21-107:8 (the NIST cybersecurity “framework does not set up any kind of requirement for them to adhere to all of the controls in 8[00-]53.”).

6. NIST 800-53 is a standard, which requires an organization to have specific controls in place in order to meet it. The NIST CSF is not; it is a voluntary self-evaluation framework.⁸

7. Following the NIST CSF does not imply that an organization meets any specific controls—including NIST 800-53 controls.⁹

8. While an organization may choose to use NIST 800-53 “as an informative reference” in evaluating itself under the NIST CSF, doing so is voluntary and does not turn the NIST 800-53 into “a checklist that must be completed” by the organization.¹⁰

9. Accordingly, whether SolarWinds followed the NIST CSF is not determined by the extent to which SolarWinds had NIST 800-53 controls in place (whether in documentation or in practice).¹¹

II. DOCUMENTS THE SEC RELIES ON AS TO THE ROLE-BASED ACCESS CONTROLS REPRESENTATION

A. June 2017 Slide Proposing More Granular Controls for Administrators’ Accounts

10. The SEC cites a slide from a deck titled “Securing Active Directory,” drafted by Brad Cline (SolarWinds’ Director of IT) and dated June 2017, well before the publication of the Security Statement and the Relevant Period. The SEC cites a slide from the deck titled “Current assessment,” which refers in part to “an unnecessary level of risk within our environment,” stating “[s]ystem team currently runs as Domain Admin.”¹²

⁸ JS ¶¶ 47, 62-63.

⁹ JS ¶ 62; Ex. 50 (Graff Dep.) 106:21-107:8 (agreeing that “following the NIST cybersecurity framework [doesn’t] infer from that that they meet any specific control”).

¹⁰ JS ¶ 63; Ex. 45 (Bliss Dep.) 84:12-15 (explaining that NIST CSF is a “voluntary framework”).

¹¹ Ex. 2 (Rattray Rep.) ¶¶ 30-39, 111; Ex. 45 (Bliss Dep.) 125:14-22 (describing NIST 800-53 as “a set of specific controls that ... are for heightened standards ...”).

¹² JS ¶ 158; Ex. 6 (SW-SEC00262012) at -013.

11. The slide does not concern any pervasive failure to implement the principle of least-privilege access or role-based access controls.¹³

12. The slide specifically related to a small team of system administrators managed by Mr. Cline.¹⁴

13. The slide was not about the team members having administrative privileges they did not need for their role. The team members were system administrators who needed administrative privileges for the systems they managed.¹⁵

14. The slide was about ideas Mr. Cline had for a more granular layer of controls that would enable the team members to use their privileged accounts only during certain tasks requiring them and to switch to non-privileged accounts for more routine operations.¹⁶

15. The ideas were based on “newer tech that was coming out” that provided for such granular controls.¹⁷

¹³ Ex. 49 (Cline Dep.) 106:12-111:22 (“[T]here were a few different folks on that team, they would have had a least-privilege model around their access levels.”), 95:17-22 (noting that assessment related to “15 accounts running as domain admin.”).

¹⁴ Ex. 49 (Cline Dep.) 95:17-22 (noting that assessment related to “15 accounts running as domain admin.”), 102:19-103:18 (discussing the “context” of this slide deck was that Cline “had just taken on the system administration team” and that this was referring to “the system administrators within that group.”), 106:2-24 (“[T]his is very specific to that team, the systems administration team[.]”), 107:1-16 (noting he was assessing access “for a select few system administrators.”), 117:12-120:10 (noting he was “just look[ing] specifically at the domain admin group”), 125:10-128:6.

¹⁵ Ex. 49 (Cline Dep.) 99:2-17 (“So the systems team in the course of their job needs domain admin to do their job[.]”), 106:12-24, 125:10-128:6 (“So this is referring to our system administrators. And removing admin rights for all roles – was not a possible technical thing for us to perform. They wouldn’t be able to do their jobs without using admin rights.”), 127:5–19 (“Their job was to be a domain administrator. ... So the idea that we could remove their domain administrative accounts means they couldn’t do their job.”).

¹⁶ Ex. 49 (Cline Dep.) 96:19-97:9 (“[S]ome recent changes within Active Directory ... gave you the ability to implement more granular controls around domain administration.”), 102:19-103:10 (discussing how “some newer technologies” allowed you to “be more granular within the systems administration team.”); 106:12-24, 107:7-108:10, 112:2-16.

¹⁷ Ex. 49 (Cline Dep.) 107:1-16 (“There were newer tech that was coming out that could allow the ability for us to apply a more granular privilege model”).

16. In other words, the slide was about an opportunity, related to a small set of employees, to refine role-based access controls that already existed, rather than a finding that role-based access controls were lacking.¹⁸

B. Documents about Efforts to Centralize and Automate Access Provisioning

1. January 2018 Slide about Evaluation of Access Management Tools

17. The SEC cites a slide deck dated January 2018 titled “User Access Management: Tool Evaluation & Recommendation,” in particular to language referring to “a collection of people who have access to many systems and many people involved in provisioning access” and a statement that “[t]he lack of standardized user access management processes that captures user provisioning ... across the organization create a loss risk of organizational assets and personal data.”¹⁹

18. The slide deck does not concern any pervasive failure to implement the principle of least-privilege access or role-based access controls.²⁰

19. The slide deck is about an evaluation of tools SolarWinds was considering using to automate the technical aspects of provisioning users with access rights.²¹

¹⁸ Ex. 49 (Cline Dep.) 95:17-22 (noting that assessment related to “15 accounts running as domain admin.”); 107:1-16.

¹⁹ JS ¶ 165; Ex. 10 (SW-SEC00043618) at -621.

²⁰ Johnson Decl. ¶ 10; Ex. 10 (SW-SEC00043618) at -621 (noting that there is no single “organization-wide standardized approach to access management,” not a lack of process generally).

²¹ Johnson Decl. ¶¶ 9-10; Ex. 46 (Brown Dep.) 208:8-14 (“So we had ... manual processes for on-boarding employees and giving them rights to certain, uh, certain systems or certain applications. And that process worked, uh, but we had not automated that process with a tool. We were going through and, uh, consolidating—we still had a Google directory service and a Azure directory service. We were consolidating to Azure.”).

20. SolarWinds had a process in place at this time for provisioning users with access based on their role—the SARF process.²²

21. However, the SARF process was relatively manual, in that implementing a SARF often required IT personnel to separately configure access rights on a number of different systems to provision the employee with access to all the systems they needed.²³

22. The more systems that IT personnel needed to separately configure, the more chances there were for errors to be made in the provisioning and deprovisioning process.²⁴

23. This slide deck was about finding an identity access and management (“IAM”) tool that would enable IT personnel to provision user access rights using one centralized system and automatically configure access rights on the downstream systems, thereby minimizing the risk of errors.²⁵

24. The Company chose to move forward with migrating to Microsoft Azure Active Directory (“Azure AD”) as its IAM tool for this purpose.²⁶

²² JS ¶ 74; Ex. 45 (Bliss Dep.) 237:21-238:7 (describing SARF process generally); Ex. 59 (Kim Dep.) 97:11-19 (noting SARF process was in place to address user access).

²³ Ex. 46 (Brown Dep.) 204:15-22 (noting that SARF was a “manual process to onboard people”); Ex. 45 (Bliss Dep.) 237:18-238:13 (same); Johnson Decl. ¶ 10.

²⁴ Johnson Decl. ¶¶ 7, 10; Ex. 45 (Bliss Dep.) 238:17-24 (“SARF—a manual process ... prone to isolated incidents such as a form not being filled out accurately or the access rights not being provisioned on a perfectly timely basis, but those were very isolated. The more you could automate that, the thought was you could reduce those isolated exceptions.”).

²⁵ Johnson Decl. ¶¶ 8-13; *see also* Ex. 49 (Cline Dep.) 69:6-19 (“We were always looking for ways to automate anything that was a manual task within IT In particular, SARF was one of the things that we had looked at as an area that we could do more automation in.”); Ex. 52 (Johnson Dep.) 103:14-21 (“Azure active directory ... was a replacement for an older technology, active directory on prem that was highly federated. The point of the identity and access management project, which put Azure AD in the cloud, was a way to centralize identity across all of the three different business units.”).

²⁶ Johnson Decl. ¶ 8; Ex. 49 (Cline Dep.) 141:14-142:4; Ex. 52 (Johnson Dep.) 102:22-103:8, 183:12-19; Ex. 46 (Brown Dep.) 209:19-210:1; Ex. 45 (Bliss Dep.) 234:3-19; Ex. 47 (Brown Inv. Vol. I) 286:17-287:24 (“[T]he process was manual. The process went through and had—it essentially worked but it had humans involved, and whenever humans are involved, it’s not as efficient and it’s not as prescriptive as what we

25. The fact that the SARF process was a relatively manual process prior to this migration being completed did not contradict the Security Statement, which did not make any representations that the Company's access provisioning process was automated in any respect.²⁷

26. The fact that SolarWinds was seeking to improve its access provisioning process does not imply that it pervasively failed to implement role-based access controls.²⁸

2. September 2018 Slide about Limited Access Management Tooling

27. The SEC also cites a September 2018 deck titled "Incident Review," which, in the appendix after the "Thank You" page, includes a slide from which the SEC quotes a line in red text stating "Identity Management – Role and Privilege Management," along with a legend indicating that red font means "Limited or non existent."²⁹

28. This text was a reference to the limited IAM and Privileged Access Management ("PAM") *tooling* at the Company, which it was seeking to remedy through the planned migration to Azure AD as well as through the rollout of a PAM tool known as "Thycotic." It was not referring to any lack of role-based access controls at the Company.³⁰

would like it to be. So this is calling out that one of the places where we need to improve is absolutely the identity management side of the world, making it more automated, making it more controlled.").

²⁷ Ex. 1 (Security Statement) at 3; Ex. 50 (Graff Dep.) 213:24-215:29-22 ("And I did double-check what you said about role-based access control. It doesn't say anything about it being automated.").

²⁸ Ex. 50 (Graff Dep.) 208:24-209:3 ("I could imagine that customers would want to move to an integrated single sign-on system for many reasons, not necessarily because their role-based control has failed.").

²⁹ JS ¶ 171; Ex. 16 (SW-SEC00386134) at -143.

³⁰ Brown Decl. ¶ 9; Ex. 46 (Brown Dep.) 208:8-14 ("So we had again manual processes for on-boarding employees and giving them rights to certain [] systems or certain applications. And that process worked, [] but we had not automated that process with a tool. We were going through and, [] consolidating – we still had a Google directory service and a Azure directory service. We were consolidating to Azure.").

3. August 2019 NIST Scorecard about Pending Migration to Azure AD and Related Notations in Later QRR Presentations

29. The SEC cites a NIST Scorecard included in an August 2019 quarterly risk review (“QRR”) presented to management.³¹ The SEC has specifically cited a bullet at the top of the slide that states: “Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures.”³² And the SEC has specifically cited the fact that this NIST Scorecard lists a “1” as the “NIST Maturity Score” for “Authentication, Authorization and Identity Management.”³³

30. Neither the cited bullet nor the “1” score concerns any pervasive failure to implement role-based access controls.³⁴

31. They are about the efforts that were ongoing at this time to improve the company’s access management processes through centralized IAM and PAM tooling, including by migrating to Azure AD and rolling out Thycotic.³⁵

³¹ JS ¶ 177; Ex. 24 (SW-SEC00001497).

³² Ex. 24 (SW-SEC00001497) at -507.

³³ Ex. 24 (SW-SEC00001497) at -507.

³⁴ Johnson Decl. ¶¶ 11-15; Ex. 49 (Cline Dep.) 141:14-142:4 (“What that’s referencing is our migration into Azure Active Directory.”); Ex. 52 (Johnson Dep.) 175:25-176:9 (“I don’t stand behind that statement. The statement was in reference to the opportunity to leverage a centralized secret server to store privileged credentials ... it was part of a presentation that ... had significantly more context.”), 181:1-186:12 (“The rationale at the time for why this was a 1 is because there was an opportunity to make an investment in Thycotic as a secret server for the entire company, and two, to make the investment in Azure AD as the authoritative source for identity and authorization for the company.”); Ex. 46 (Brown Dep.) 209:19-210:1 (“At that point in time we had Google and Azure. So consolidating those to make Azure our—our source.”); Ex. 45 (Bliss Dep.) 234:3-19 (explaining that score of “1” was “subjective determination” in order to “[g]enerate[] a conversation in this venue.”).

³⁵ Johnson Decl. ¶ 15; Ex. 52 (Johnson Dep.) 181:1-186:12 (“The rationale at the time for why this was a 1 is because there was an opportunity to make an investment in Thycotic as a secret server for the entire company, and two, to make the investment in Azure AD as the authoritative source for identity and authorization for the company.”); Ex. 46 (Brown Dep.) 209:19-210:1 (explaining “movement to make Azure Active Directory the authoritative only source.”); Ex. 45 (Bliss Dep.) 234:3-19.

32. Another bullet on the Scorecard specifically references the Azure AD project, stating: “Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets.”³⁶

33. A draft of this Scorecard reflects that the “KPI” (key performance indicator) driving the “1” score was the “[n]umber of assets (mission/business critical) with AD Authentication enabled vs. not enabled”—*i.e.*, the number of systems that had been integrated with Azure AD to date as part of this project.³⁷

34. Moving from manual to automated processes is a common way that companies mature their cybersecurity controls under the NIST CSF.³⁸

35. The migration to Azure AD was a complex, multi-year project that SolarWinds pursued during the Relevant Period.³⁹

36. The “1” score was intended to convey to management (the audience for NIST Scorecards) that the migration to Azure AD was an important opportunity to mature the Company’s access management processes but that it was still in progress and needed continued support and resourcing.⁴⁰

³⁶ Ex. 24 (SW-SEC00001497) at -507.

³⁷ Johnson Decl. ¶ 15; Ex. 35 (SW-SEC00623600) at -609.

³⁸ Ex. 2 (Rattray Rep.) ¶ 154; Ex. 50 (Graff Dep.) 216:22-217:1 (agreeing that “one way a company can mature its controls is by making them more automated and more centralized”).

³⁹ Johnson Decl. ¶ 13; Ex. 59 (Kim Dep.) 275:8-17 (noting that “obviously migrating your identity service to a single service actually takes a very long time”).

⁴⁰ Johnson Decl. ¶¶ 13-15; Ex. 49 (Cline Dep.) 141:14-142:4 (“What that’s referencing is our migration into Azure Active Directory.”); Ex. 52 (Johnson Dep.) 175:25-176:9 (“I don’t stand behind that statement. The statement was in reference to the opportunity to leverage a centralized secret server to store privileged credentials ... it was part of a presentation that ... had significantly more context.”), 181:1-186:12 (“The rationale at the time for why this was a 1 is because there was an opportunity to make an investment in Thycotic as a secret server for the entire company, and two, to make the investment in Azure AD as the authoritative source for identity and authorization for the company.”); Ex. 46 (Brown Dep.) 209:19-210:1 (“At that point in time we had Google and Azure. So consolidating those to make Azure our—our source.”);

37. The ongoing rollout of Azure AD is also what is referred to in notations the SEC cites from subsequent QRR presentations, including:

a. a note from a November 2019 QRR presentation stating “Pushing forward with AD authentication guidelines for critical mission systems”,⁴¹

b. notes from a March 2020 QRR presentation and May 2020 QRR presentation referencing enforcement of “AD authentication” among improvements being made;⁴² and

c. a note from an October 2020 QRR presentation stating “Continue to enable AD Authentication for critical systems.”⁴³

C. March 2020 Slide about User Access Review for SOX Audit

38. The SEC cites a note in a slide in a March 2020 QRR presentation stating: “Significant deficiencies in user access management.”⁴⁴

39. This note does not concern any pervasive failure to implement the concept of least-privilege access or role-based access controls.⁴⁵

Ex. 45 (Bliss Dep.) 234:3-19 (explaining that score of “1” was “subjective determination” in order to “[g]enerate[] a conversation in this venue.”).

⁴¹ Ex. 28 (SW-SEC00001551) at -552.

⁴² Ex. 37 (SW-SEC00001608) at -611; Ex. 38 (SW-SEC00001602) at -605.

⁴³ Ex. 40 (SW-SEC00001582) at -587.

⁴⁴ JS ¶¶ 181, 197; Ex. 37 (SW-SEC00001608) at -611.

⁴⁵ Johnson Decl. ¶¶ 16-18; Ex. 46 (Brown Dep.) 237:21-24 (explaining that note “isn’t a finding. This is simply a statement.”); Ex. 52 (Johnson Dep.) 222:3-223:10 (“That was specifically in response to a user access review ... so in user access reviews under SOX controls, you are able to define quarterly what the user community that needs to be audited for, whether or not the access is appropriate and that access has been terminated for people who no longer have acquired that access ... What I was calling out ... is that our user access reviewer didn’t understand ... how to define the user access review period ... That was caught before external auditors reviewed and the internal audit was rerun.”).

40. The note referred to a mistake made in conducting user access reviews in preparation for the Company's 2020 SOX audit: the reviews were run across the wrong window of time, resulting in a significant number of users being erroneously excluded from the review.⁴⁶

41. The note used "significant deficiencies"—a SOX term—loosely, to refer to this SOX-related issue.⁴⁷

42. However, the issue was internally discovered and fixed (by re-running the user access reviews in question) before the completion of the Company's actual SOX audit and did not result in any significant deficiency finding by the Company's auditors.⁴⁸

43. The "[s]ignificant deficiencies" note in the March 2020 QRR also appears in later QRRs cited by the SEC and refers to the same one-time problem with how user access reviews were initially conducted in preparation for the 2020 SOX audit. The repetition was simply a result of not changing the slide from one iteration of the QRR to the next, and was not intended to indicate any more extensive or continuing problem the Company had regarding access management.⁴⁹

D. "Preliminary Review" Relating to FedRAMP Certification

44. The SEC cites three emails from June, August, and September 2019 attaching a spreadsheet described as "a preliminary review of the 325 FedRAMP Moderate controls," which

⁴⁶ Johnson Decl. ¶¶ 23-24; Ex. 52 (Johnson Dep.) 222:6-225:11 ("What I was calling out ... is that our user access reviewer didn't understand ... how to define the user access review period properly ... So there was deficiency in user access population that was used to do the user access review.").

⁴⁷ Johnson Decl. ¶¶ 23-25; Ex. 52 (Johnson Dep.) 222:6-222:17 ("[S]o in user access reviews under SOX controls, you are to define quarterly what the user community that needs to be audited for ..."); Campbell Decl. ¶ 4.

⁴⁸ Johnson Decl. ¶ 24; Ex. 52 (Johnson Dep.) 222:6-225:11, 226:3-15 ("The issue was remediated once detected [sic]—all of the teams had to rerun their user access reviews. It was remediated before the external audit").

⁴⁹ JS ¶¶ 182-83; 198; Ex. 39 (SW-SEC00148267) at -270; Ex. 38 (SW-SEC00001602) at -605; Ex. 40 (SW-SEC00001582) at -587; Campbell Decl. ¶¶ 10-12; Johnson Decl. ¶ 25.

assessed “what resources are needed for a FedRAMP effort” in connection “with the upcoming 2020 budget cycle.”⁵⁰

45. The emails were sent, and the spreadsheet was prepared, by Kellie Pierce, a program manager at SolarWinds who worked under Rani Johnson and Tim Brown.⁵¹

46. “FedRAMP” refers to a type of certification that cloud software must have in order to be sold to the federal government.⁵²

47. FedRAMP certification requires meeting a highly demanding set of controls, which must be established through documentation validated by a third-party assessor.⁵³

48. Ms. Pierce’s spreadsheet was prepared as part of a preliminary attempt to estimate how much effort it would require for SolarWinds to achieve FedRAMP certification for its cloud products.⁵⁴

⁵⁰ JS ¶¶ 174-76; Ex. 22 (SW-SEC00151673) at -673; Ex. 25 (SW-SEC00045356) at -356; Ex. 27 (SW-SEC00218068).

⁵¹ Ex. 56 (Pierce Dep.) 46:19-49:25.

⁵² Ex. 2 (Rattray Rep.) ¶ 142 (“FedRAMP is a highly demanding set of federal standards that cloud products must meet for the federal government to be able to purchase them.”); Johnson Decl. ¶¶ 19-20; Ex. 52 (Johnson Dep.) 203:1-9 (“[T]hat’s one of the very foundational components of [F]edRAMP readiness, is that the access to the information systems that are being provided to the U.S. federal government.”).

⁵³ Johnson Decl. ¶ 20; Ex. 50 (Graff Dep.) 241:24-242:1 (agreeing that FedRAMP “is a pretty demanding standard for companies to meet”); Ex. 52 (Johnson Dep.) 194:19-196:2 (“It was a very cursory collection of data ... because the formality and the requirement of leveraging a third-party assessment organization or a [third-party auditing organization] for [F]edRAMP is very expensive and you have to create years—at least a year of reporting documentation. ... What’s more, the—there was ... a hypothesis on Kellie’s part and certainly mine because she and I have run programs before to prepare companies for product certifications.”); Ex. 56 (Pierce Dep.) 125:19-23.

⁵⁴ Ex. 56 (Pierce Dep.) 48:3-5 (explaining that this was “a preliminary, very beginning, like, quick and dirty-type evaluation to see if the company wanted to invest in FedRAMP certification”); Ex. 52 (Johnson Dep.) 194:13-16 (“This was a preliminary reaction to a request to make an investment in [F]edRAMP readiness for products that did not have a strong business justification.”); Ex. 45 (Bliss Dep.) 186:2-5 (explaining that the objective was to do a “quick, cursory, preliminary review as to how much do we think this is going to cost us? How much effort needs to go into this?”), 186:8-14 (explaining Ms. Pierce was “more or less spitballing” to create a budget estimate); Johnson Decl. ¶¶ 21-22.

49. Ms. Pierce’s takeaway from the preliminary review was that it would take a moderate to significant level of effort to implement most of the FedRAMP controls.⁵⁵

50. Ms. Pierce’s preliminary review was not about whether SolarWinds had implemented the policies described in the Security Statement.⁵⁶

51. The Security Statement says nothing about whether SolarWinds had FedRAMP controls in place.⁵⁷

52. FedRAMP controls are much more extensive and demanding than the policies described in the Security Statement, including with respect to access controls.⁵⁸

53. FedRAMP controls also generally focus on the security of the cloud products being certified rather than the vendor’s cybersecurity program more broadly.⁵⁹

54. For example, many FedRAMP controls specifically reference the term “information system”—which is a reference to the cloud product being certified and used by the federal government, rather than the vendor’s corporate network.⁶⁰

⁵⁵ Johnson Decl. ¶ 22; Ex. 52 (Johnson Dep.) 187:1-203:24 (confirming that the cost of achieving FedRAMP certification would exceed any benefits to SolarWinds).

⁵⁶ Ex. 52 (Johnson Dep.) 192:10-18 (“Kellie’s ask is to provide a summary of level of effort to prepare for [F]edRAMP readiness that is two years out. It’s not an assessment of alignment with controls.”).

⁵⁷ Ex. 1 (Security Statement).

⁵⁸ Compare Ex. 22 (SW-SEC00151673) at pdf p. 5-9 (excerpt of spreadsheet of FedRAMP controls setting forth 45 detailed controls relating to access controls, spanning five pages in small font), with Ex. 1 (Security Statement) at 3 (short section describing basic role-based access controls); Ex. 2 (Rattray Rep.) ¶ 145; see also Ex. 50 (Graff Dep.) 241:24-242:1 (“Q. And you’re aware Fed Ramp is a pretty demanding standard for companies to meet? A. Yes, I’d agree.”).

⁵⁹ Ex. 2 (Rattray Rep.) ¶¶ 142, 145 (“[M]any of the requirements relate to access controls on the cloud product at issue rather than access controls on SolarWinds’ network.”); Ex. 22 (SW-SEC00151673) at pdf p. 5-9, column J (containing Ms. Pierce’s categorization of each control as either relating to “Process,” “Product,” or “People,” with most categorized as “Product”); Ex. 50 (Graff Dep.) 242:2-6 (“Q. ... [T]he certification is for particular cloud products, right, that’s what Fed Ramp is for? You have to have that certification to sell a cloud product to the federal government? A. Yes, that’s right.”).

⁶⁰ Ex. 22 (SW-SEC00151673) at pdf p. 7, line 23 (FedRAMP control requiring that “the information system” display a banner at logon advising users that they “are accessing a U.S. government information

55. Therefore, Ms. Pierce’s conclusion that many FedRAMP controls were not in place at the Company does not imply that the representations in the Security Statement were untrue.⁶¹

56. In any event, Ms. Pierce’s preliminary review was not a reliable assessment even with respect to FedRAMP controls.⁶²

57. Ms. Pierce was asked to conduct the preliminary review not as a security exercise, but as a budgeting exercise.⁶³

58. SolarWinds’ cloud software business line wanted to be able to sell its products to the federal government.⁶⁴

59. Rani Johnson, SolarWinds’ Chief Information Officer, did not believe the benefit of being able to sell the federal government SolarWinds’ cloud products—which comprised a small portion of SolarWinds’ overall business—would be worth the effort required to achieve FedRAMP certification for the products.⁶⁵

system”); Ex. 50 (Graff Dep.) 246:20-247:8 (“So the information system being referred to here would be the cloud product that is being sold, which needs to inform users of that product that they’re accessing a U.S. government system? A. That’s a—that’s a reasonable interpretation. ... Q. So it’s possible that when you have a number of controls in here to talk about what the information system has to do, it’s not talking about SolarWinds network or the organization as a whole, but whatever cloud product is being evaluated for Fed Ramp purposes? A. There’s one of them that might well qualify that way.”).

⁶¹ Ex. 2 (Ratray Rep.) ¶ 145.

⁶² Ex. 56 (Pierce Dep.) 21:17-18 (“I’m not a technical person.”), 47:16-17 (“I’m also not a FedRAMP expert. So I’m not 100 percent sure.”), 125:19-23 (agreeing she did not “have a good technical understanding of what [the] language in the [FedRAMP] technical controls actually meant”); Ex. 52 (Johnson Dep.) 192:10-18 (“Kellie is not an auditor and has no expertise in this particular area.”), 194:12-196:3; Johnson Decl. ¶¶ 21-22.

⁶³ Johnson Decl. ¶ 22; Ex. 2 (Ratray Rep.) ¶ 142; Ex. 56 (Pierce Dep.) 75:21-76:11 (identifying Ex. 27 (SW-SEC00218068) as “a quantified estimate for the amount of budget we would need if we wanted to move forward with the FedRAMP certification.”).

⁶⁴ Ex. 45 (Bliss Dep.) 184:20-186:14 (“And as we looked at the cloud products, the question became, what do we need to sell those products to our customer base of which some of that was government customers?”).

⁶⁵ Ex. 52 (Johnson Dep.) 194:19-196:2 (“The reality that these products don’t have the U.S.-based staffing infrastructure [required under FedRAMP] means that we knew that we would ... this would be too [expensive] of an effort. So this was a very cursory, very preliminary [stab] at [showing] this is gonna cost

60. So Ms. Johnson asked Ms. Pierce to do a “very cursory” review of FedRAMP controls to come up with a rough estimate of the effort required.⁶⁶

61. Ms. Pierce was a program manager who worked under Ms. Johnson, whose entire role at the company was a coordination role.⁶⁷

62. Ms. Pierce did not have technical security expertise.⁶⁸

63. Ms. Pierce lacked a good understanding of what the language in the FedRAMP controls meant.⁶⁹

64. In reviewing the FedRAMP controls, Ms. Pierce took “basically [her] best guess” as to whether SolarWinds had them in place.⁷⁰

too much and not going to be worth the effort in this time frame.”); Ex. 45 (Bliss Dep.) 35:4-13 (describing cloud product line as “a very small business group”); Johnson Decl. ¶ 22.

⁶⁶ Ex. 52 (Johnson Dep.) 194:13-196:2 (“The ask here is truly to do a level-of-effort estimate around how much work we need to prepare to create the reporting documentation to ready those assets for [F]edRAMP so we can—say, if this cost 2 million, how much in sales is there to potentially justify this investment. ... So this was a very cursory, very preliminary [stab] at this is gonna cost too much and not going to be worth the effort in this time frame.”), 202:18-21 (“So my conversations with her were about how much effort to spend because we had a hypothesis that the answer would be the company would not make this investment.”); Ex. 56 (Pierce Dep.) 47:18-48:5 (“Q. And what was your involvement in the—assessing FedRAMP moderate controls, if any? A. Again, a coordination role ...”).

⁶⁷ Ex. 56 (Pierce Dep.) 87:10-11 (“Similar to pretty much my entire role at SolarWinds. It would have been a coordination role.”), 47:16-48:5; Ex. 45 (Bliss Dep.) 32:20-25.

⁶⁸ Ex. 56 (Pierce Dep.) 21:17-18, 28:18-19 (“As I stated before, I’m not a technical person.”); Ex. 57 (Pierce Inv. Vol. I) 176:23-24 (“I would coordinate the reports, but I’m not a technical person ...”), 181:21 (“As I stated earlier I’m not highly technical ...”); Ex. 45 (Bliss Dep.) 32:20-25 (“Kellie’s role was more to make sure that the trains were running on time, that notes were taken accordingly, that materials were produced. She wasn’t a technical resource.”); Johnson Decl. ¶ 21.

⁶⁹ Ex. 56 (Pierce Dep.) 47:16-17 (“I’m also not a FedRAMP expert.”); Ex. 52 (Johnson Dep.) 192:14-15 (“Kellie is not an auditor and has no expertise in this particular area”).

⁷⁰ Ex. 56 (Pierce Dep.) 28:13-25, 60:10-19.

65. She based her guesses on reading the language in each control and seeing if she recalled seeing similar language in SolarWinds policy documentation she had reviewed in the past, through coordinating SOC-2 audits the Company had completed.⁷¹

66. Ms. Pierce's comments in her preliminary review were never validated by anyone else for accuracy.⁷²

67. The only FedRAMP control evaluated in the preliminary review that resembles a representation made in the Security Statement concerning access controls is a control stating: "The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."⁷³

68. In the spreadsheet she prepared, Ms. Pierce marked this as a control SolarWinds "may have" in place and placed a comment stating: "This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed."⁷⁴

69. The comment was inaccurate, as SolarWinds' systems had been audited previously against the principle of least privilege.⁷⁵

⁷¹ Ex. 56 (Pierce Dep.) 49:8-17, 55:3-56:1 ("Again, this was a very preliminary, you know, just a request that we—that we got to do turnaround pretty quickly, so I made my best guess based on what—what I had seen in the SOC 2 or the ISO 27001 audits."), 124:22-125:18 ("Q. Did you rely on anything other than your memory of those policies based on your limited experience coordinating SOC 2 and ISO audits? A. No, I did not.").

⁷² Ex. 56 (Pierce Dep.) 50:8-17; Ex. 52 (Johnson Dep.) 194:12-195:10, 196:16-23.

⁷³ Ex. 2 (Rattray Rep.) ¶ 146; Ex. 22 (SW-SEC00151673) at pdf p. 7, line 16.

⁷⁴ Ex. 22 (SW-SEC00151673) at pdf p. 7, line 16.

⁷⁵ Ex. 2 (Rattray Rep.) ¶ 147 ("SolarWinds *did* audit its compliance with the least privilege principle, through the user access reviews that it regularly conducted, which looked specifically at what level of privilege each user in the company had."); Ex. 3 (Graff Rep.) ¶¶ 61, 97 & n.180 (referencing certain audits for least privilege).

E. Engineer's Concerns about Employees Using Personal Laptops on VPN

70. The SEC cites emails in which Róbert Krajčír, a network engineer, conveyed concerns he had about the fact that SolarWinds employees and contractors could use their personal laptops to remotely log into their SolarWinds accounts through the Company's VPN—a practice commonly referred to as “Bring Your Own Device” or “BYOD.”⁷⁶

71. Mr. Krajčír's concerns regarding BYOD did not concern role-based access controls or the principle of least privilege.⁷⁷

72. Mr. Krajčír's concerns instead were about SolarWinds' ability to monitor user personal devices connected to the network—for example, to monitor whether the devices might be infected with malware.⁷⁸

73. The Security Statement section on role-based access controls does not say anything about the Company's BYOD policies or whether users were required to connect to the Company's network from a company-managed device.⁷⁹

F. August 2017 Budget Request and October 2018 Draft Update

74. The SEC cites a slide deck for SolarWinds' Monthly IT Leadership Meeting in August 2017.⁸⁰

⁷⁶ JS ¶¶ 166, 168-69, 180; Ex. 14 (SW-SEC00031653) at -657; Ex. 15 (SW-SEC00594395) at -395; Ex. 34 (SW-SEC00666779) at -779; Krajčír Decl. ¶ 5.

⁷⁷ Krajčír Decl. ¶ 6; Ex. 49 (Cline Dep.) 183:18-184:9 (explaining that Krajčír was “referring to attempting to implement certificates on devices joining our VPN to remove the potential for unmanaged devices.”).

⁷⁸ Krajčír Decl. ¶¶ 7-8; Ex. 49 (Cline Dep.) 191:9-25, 192:18-197:3 (“So to be clear, he's talking about administrative rights on your local device.”).

⁷⁹ Krajčír Decl. ¶¶ 4, 6; Ex. 1 (Security Statement) at 3.

⁸⁰ JS ¶¶ 159-60; Ex. 7 (SW-SEC00259782) at -787-88.

75. The slide deck includes a \$660,000 budget request from Mr. Brown—earmarked for additional personnel, security tools, and training for employees.⁸¹

76. Next to the budget request, under the heading “Risks of Non-Investment,” Mr. Brown included a bullet point stating: “Current state of security leaves us in a very vulnerable state for our critical assets.”⁸²

77. This language was merely hyperbole intended to underscore the importance of investing in cybersecurity and increase the likelihood his budget request would be granted.⁸³

78. The language was likewise understood by the audience for the presentation to be jargon Mr. Brown was using to make a business case for the budget request, as opposed to a specific factual finding.⁸⁴

79. The language was not intended to convey that SolarWinds was pervasively failing to implement role-based access controls (or any other practices described in the Security Statement).⁸⁵

⁸¹ Ex. 7 (SW-SEC00259782) at -788.

⁸² Ex. 7 (SW-SEC00259782) at -788.

⁸³ Brown Decl. ¶¶ 3-5; Ex. 46 (Brown Dep.) 157:10-13, 160:6-7.

⁸⁴ Ex. 45 (Bliss Dep.) 216:20-217:8 (“My understanding of that statement, first, is that it was attached originally to a budget request being made. So as with any budget request, there's a certain amount of hyperbole that's introduced....”); Ex. 52 (Johnson Dep.) 139:2-11 (“I don’t know what Tim was intending by these statements. However, the purpose of the 2017 document ... was to make a business case. Business case justifications are generally jargon or summarized nonprecise language to make a point to make investment.”), 141:7-142:10 (“The statements he was making in a slide deck to his boss and to make a business justification weren’t a statement of status or qualified in any way. It was merely meant to make a business justification. ... [The language] is not accurate.”).

⁸⁵ Brown Decl. ¶¶ 3-5, 21; Ex. 46 (Brown Dep.) 157:2-15 (explaining that the language was part of an “attempt[] to support my budget request”); Ex. 45 (Bliss Dep.) 220:4-221:5 (“I do not think this is a factual finding.”); Ex. 52 (Johnson Dep.) 139:13-21 (“It’s not intended to make a statement on the status of security; it’s to make a request to invest.”), 141:12-14 (“That statement is imprecise and not accurately reflecting—it is a business case justification, like, of a problem statement.”).

80. The SEC cites slide decks from September 2017 and December 2017 that include a copy of Mr. Brown’s budget request from the August 2017 presentation, containing the same language.⁸⁶

81. The repetition of the budget request in these slide decks is simply a result of the information being copied into similar slide decks—it does not represent any repeated “findings” by Mr. Brown.⁸⁷

82. The SEC also cites a draft slide deck emailed from Mr. Brown to Rani Johnson on October 29, 2018, titled “Information Security - Risk review October 2018.”⁸⁸

83. Mr. Brown stated in the email that the draft included “[a] review of what we asked for last August and a red yellow green status showing how we have done on our initiatives. ... We can review in tomorrow but it’s a reasonable place to start.”⁸⁹

84. The draft included two copies of Mr. Brown’s budget request from August 2017—one as it originally appeared, and a second copy labeled “Updated October 2018 with status,” with the font color of some of the language from the original budget request changed to either red, yellow, or green. The language “Current state of security leaves us in a very vulnerable state for our critical assets” was changed to yellow font in the second copy of the slide.⁹⁰

85. All Mr. Brown meant to convey by yellow font is that improvements had been made since August 2017, but there was still work to be done.⁹¹

⁸⁶ JS ¶¶ 161-64, 172-73; Ex. 8 (SW-SEC00337355) at -360; Ex. 9 (SW-SEC00262716) at -743.

⁸⁷ Brown Decl. ¶ 6.

⁸⁸ JS ¶ 173; Ex. 19 (SW-SEC00313350) at -351.

⁸⁹ Ex. 19 (SW-SEC00313350) at -350.

⁹⁰ Ex. 19 (SW-SEC00313350) at -359, -361.

⁹¹ Brown Decl. ¶ 7; Ex. 46 (Brown Dep.) 167:3-168:5 (“[Y]ellow indicates that some of it was done and we could do more ... certain improvements had been done and there were still more to do.”).

86. Ms. Johnson’s reaction to the draft was that it was “not the way we would formally represent completion or risk” or the “status of initiatives,” and thus the draft would not have been finalized in this form (if it was ever finalized).⁹²

III. DOCUMENTS THE SEC RELIES ON AS TO THE PASSWORD REPRESENTATION

A. March 2018 Slide about Progress on User Account Audit

87. The SEC cites a slide in a draft slide deck attached to an email in March 2018, containing a progress report on a project titled “Enterprise Access Management (Standards & Audit).” The SEC cites in particular two notations in the lower left corner of the document, under “Issues, Risks & Dependencies,” stating: “Concept of least privilege not followed as a best practice” and “Use of shared accounts throughout internal and external applications.”⁹³ The SEC cites this same language that was copied into a May 2019 slide deck.⁹⁴

88. This project concerned an audit of user accounts that was conducted in late 2017, approximately a year before the Relevant Period.⁹⁵

89. The notation “Concept of least privilege not followed as a best practice” refers to the “issue” the audit was looking into—*whether* the concept of least privilege was not being followed as a best practice on the audited systems, as reflected in the project components listed on

⁹² Ex. 52 (Johnson Dep.) 133:9-134:12 (“This is not the way we would formally represent completion or risk. It is likely why Tim wanted to meet. ... The DOIT organization presented monthly status of all initiatives. This is not the format for the presentation of status of initiatives. ... And so I would have worked with him to finalize this in a consistent manner with our artifacts.”), 139:2-25 (“[T]he purpose of the 2017 document that was updated in 2018 with Tim Brown’s color coding was to make a business case. Business case justification are generally jargon or nonprecise language to make a point to make investment.”), 140:16-17 (“It’s a business case document using nonprecise terms to make the point to invest.”).

⁹³ JS ¶ 184; Ex. 13 (SW-SEC00042892) at -907.

⁹⁴ JS ¶ 178; Ex. 26 (SW-SEC00001635) at -644; Campbell Decl. ¶¶ 13-14.

⁹⁵ Ex. 2 (Rattray Rep.) ¶ 137; Ex. 54 (Quitugua Dep.) 202:13-203:10; Campbell Decl. ¶¶ 13-14.

the other side of the slide (*e.g.*, “Conduct risk audit and risk assessment against privileged and non-privileged user accounts”).⁹⁶

90. As testified by Eric Quitugua, who was the lead for the project listed on the slide, the notation “doesn’t indicate” there was any “problem across the organization.”⁹⁷

91. “As part of the assessment, it may have been found that a particular system wasn’t following the concept of least privilege.”⁹⁸ But to the extent any non-compliant systems were identified, they would have been remediated as part of the audit.⁹⁹

92. Another “issue” the audit covered was checking internal and external applications for the use of shared accounts.¹⁰⁰

93. Specifically, as Mr. Quitugua explained, the audit was focused on *service accounts*, which are accounts intended for use by an application, rather than individual users. For example, if an application needs to look up information from a database, it may need an account on that database to be able to do so. That account is called a “service account.”¹⁰¹

⁹⁶ Ex. 54 (Quitugua Dep.) 219:14-22 (“The issue, risk and dependencies listed here, doesn’t indicate that it was a problem across the organization.”); Ex. 13 (SW-SEC00042892) at -907; Ex. 2 (Ratray Rep.) ¶ 137.

⁹⁷ Ex. 54 (Quitugua Dep.) 219:14-24; Ex. 2 (Ratray Rep.) ¶¶ 138-39.

⁹⁸ Ex. 54 (Quitugua Dep.) 219:14-24.

⁹⁹ Ex. 54 (Quitugua Dep.) 219:14-220:10 (“[W]e do have those kind of defined steps to go through to identify, take in the reports and then address and fix.”); Ex. 50 (Graff Dep.) 203:22-204:5 (agreeing that audits are meant “to make sure everything is going well and if there’s things that are not going well to identify them for mitigation[.]”).

¹⁰⁰ Ex. 55 (Quitugua Inv. Vol. II) 291:25-293:2 (explaining that the intent of the project was “to work with teams to decommission the use of those shared accounts,” by first identifying shared accounts and determining if they were needed by the application, and then “rotat[ing] the credentials” for the accounts so “they couldn’t be used as shared”).

¹⁰¹ Ex. 55 (Quitugua Inv. Vol. II) 289:20-290:21 (explaining that “service accounts” were “used to run automated scripting processes within the business applications”); Ex. 54 (Quitugua Dep.) 221:8-23 (explaining that a “shared account ... can be used by a computer to perform its function”); Ex. 2 (Ratray Rep.) ¶ 162.

94. Prior to conducting the audit, Mr. Quitugua had discovered instances where service accounts intended for use by an application were being used by individual members of the relevant application team in the course of their work, which was not best practice.¹⁰²

95. As part of the audit, Mr. Quitugua undertook an effort to identify any service accounts used in this way and decommission them wherever found.¹⁰³

96. The slide identifies Q1 2018 as the completion date for the work, which is well before the Relevant Period.¹⁰⁴

97. Auditing policies to find and remediate gaps is a means of enforcing those policies.¹⁰⁵

98. This audit was part of SolarWinds' efforts to enforce the principle of least privilege and a policy against the use of shared accounts.¹⁰⁶

99. In any event, the Security Statement itself does not make any representation that SolarWinds employees never use shared accounts. It merely states that SolarWinds requires that

¹⁰² Ex. 5 (Quitugua Inv. Vol. II) 289:20-290:21 (“What we found was that these service accounts, which were purpose built to run processes, were also being used by, you know, users, and they also knew the credentials, right. So that case, we considered those accounts shared accounts, accounts that users should not have access to ...”); Ex. 2 (Rattray Rep.) ¶¶ 162-63.

¹⁰³ Ex. 55 (Quitugua Inv. Vol. II) 291:25-293:2 (explaining that the intent of the project was “to work with teams to decommission the use of those shared accounts,” by first identifying shared accounts and determining if they were needed by the application, and then “rotat[ing] the credentials” for the accounts so “they couldn’t be used as shared”); Ex. 2 (Rattray Rep.) ¶¶ 162-63.

¹⁰⁴ Ex. 13 (SW-SEC00042892) at -907.

¹⁰⁵ Ex. 2 (Rattray Rep.) ¶ 171 (“Identifying and remediating discrepancies is what an audit is conducted for ...”).

¹⁰⁶ *Id.*; *see also id.* ¶ 130 (“As I know from my experience as a CISO at a large organization, this is what a well-functioning cybersecurity program does on a daily basis: It has general processes in place, but is always on the lookout for specific areas where those processes can be improved.”), ¶ 163 (“That is exactly what you would expect a well-functioning cybersecurity program to do in order to *enforce* a policy against sharing of accounts: identify a gap, investigate it further, and remediate it.”).

employees be “provisioned with unique account IDs,” which was in fact the Company’s routine practice.¹⁰⁷

B. November 2019 Emails about Developer Access to Billing Data

100. The SEC cites a November 2019 email chain, in which an employee stated that certain software developers “are currently using a shared login currently of a different SolarWinds employee. This is definitely a security incident and needs to stop. Solution – Granting the individual logins as requested.”¹⁰⁸

101. The software developers were working on improvements to the billing system used by SolarWinds’ Finance Department.¹⁰⁹

102. To complete that task, the developers needed access to the billing data.¹¹⁰

103. To access the billing data required having SuperUser access on the relevant billing system.¹¹¹

¹⁰⁷ Ex. 1 (Security Statement) at 3; Ex. 2 (Ratray Rep.) ¶ 160 (“The Security Statement does not purport to guarantee that sharing of accounts never occurred at SolarWinds. Instead it merely states that SolarWinds ‘require[s] that authorized users be provisioned with unique account IDs.’”), ¶169 (same).

¹⁰⁸ JS ¶ 186; Ex. 29 (SW-SEC00254254) at -265.

¹⁰⁹ Ex. 29 (SW-SEC00254254) at -258; Ex. 2 (Ratray Rep.) ¶ 122.

¹¹⁰ Ex. 29 (SW-SEC00254254) at -265 (explaining that “we were developing billing using production services since the beginning as only production has data to test billing”), -264 (explaining it would require engineering effort to obtain “enough test data” without “going to production” for it), -260 (explaining that the issue was “how best to secure access to production data in order to improve our billing systems”); Ex. 2 (Ratray Rep.) ¶ 122; Ex. 50 (Graff Dep.) 161:22-162:2 (“Q. The developers thought they needed [access to] it, right? A. Either the developers or their manager.”), 171:16-22 (“Q... . The principle [of role-based access] is employees getting access based on what they need to do for their role. Here there was a determination made that, in order to perform their role, they needed this access at the time. The company was entitled to make that determination, was it not? A. Yes.”), 173:8-11 (“There was one specific group of people that needed access, were declared to have needed access, and they were given read-write access using shared log-ins on live production data ...”), 174:1-8 (“Yes, and they needed read access for their jobs. ... The company is within its right to make that exception to the role-based access controls.”).

¹¹¹ Ex. 29 (SW-SEC00254254) at -262-63; Ex. 50 (Graff Dep.) 162:1-2; Ex. 2 (Ratray Rep.) ¶¶ 122-24.

104. Because the developers lacked such access on the system, they initially borrowed the credentials of a different SolarWinds employee with SuperUser access.¹¹²

105. This was flagged as a security violation, which led to the developers requesting SuperUser access for themselves.¹¹³

106. The request was evaluated and approved by Mr. Brown and other security personnel.¹¹⁴

107. This event does not reflect that SolarWinds had a policy or practice of permitting employees to share accounts.¹¹⁵

108. The fact that the developers' borrowing of someone else's account was flagged as a security violation when it was discovered reflects that SolarWinds had a policy of prohibiting employees from sharing accounts.¹¹⁶

C. November 2019 Discovery and Remediation of “solarwinds123” Password

109. The SEC cites emails concerning a security researcher's report through which SolarWinds was alerted to and remediated a password—“solarwinds123”—on a third-party system, which did not meet the Company's password complexity requirements.¹¹⁷

¹¹² Ex. 29 (SW-SEC00254254) at -265 (explaining that the developers were “using a shared login currently of a different SolarWinds employee,” which “needs to stop”), -255 (explaining that the developers were using “shared logins with Superuser access to Production Backup data in order to pull data for billing” through two different APIs); Ex. 2 (Ratray Rep.) ¶ 122.

¹¹³ Ex. 29 (SW-SEC00254254) at -257, -265-66; Ex. 2 (Ratray Rep.) ¶ 122.

¹¹⁴ Ex. 43 (SW-SEC00168780) at pdf p. 3 (“Risk reviewed and accepted by Tim Brown”).

¹¹⁵ Ex. 50 (Graff Dep.) 172:16:21 (“Q. ... So you can't infer from this e-mail that SolarWinds' systems were pervasively designed to give everyone read and write access; you're not drawing that conclusion, are you? A. No. There are other conclusions I'm drawing from it, but not that one.”), 174:9-14 (“Q. [Y]ou're not contending that this shows that SolarWinds just pervasively granted everybody read/write access to all their systems; this was a single exception related to a particular team and a particular system? A. This particular incident, yes.”); Ex. 2 (Ratray Rep.) ¶¶ 123-25.

¹¹⁶ Ex. 2 (Ratray Rep.) ¶¶ 123-25, 166-67.

¹¹⁷ JS ¶¶ 187, 189; Ex. 30 (SW-SEC00001464); Ex. 31 (SW-SEC00001476) at -484.

110. The password was for a single account on a single server hosted by Akamai, a third-party service provider (the “Akamai Server”).¹¹⁸

111. While SolarWinds’ routine practice was to enforce password complexity requirements automatically on systems that provide for such functionality, the Akamai Server did not provide functionality that would have allowed SolarWinds to enforce its password complexity requirements.¹¹⁹

112. As a result, SolarWinds had to rely on manual compliance with the company’s password complexity requirements with respect to the Akamai Server, which is always subject to the possibility of human error.¹²⁰

113. There is no evidence of any other non-complex passwords being used within SolarWinds during the Relevant Period or any evidence otherwise indicating that the use of non-complex passwords was a frequent problem at the Company.¹²¹

¹¹⁸ Ex. 31 (SW-SEC00001476) at -483; Ex. 50 (Graff Dep.) 250:20-251:3; Ex. 2 (Rattray Rep.) ¶¶ 175-77.

¹¹⁹ Ex. 2 (Rattray Rep.) ¶ 175; Ex. 52 (Johnson Dep.) 247:9-13 (discussing an analysis of “whether or not the product themselves can enforce password complexity control” where “[t]hose products are not part of the IT infrastructure for password management”); Zimmerman Decl. ¶ 6 (“[I]t is only possible to enforce password complexity automatically on systems that provide that functionality. SolarWinds did not have the ability to automatically enforce its password requirements on the Akamai Server,” which “did not have any functionality that enabled SolarWinds to automatically enforce its password complexity requirements on user accounts.”); Ex. 50 (Graff Dep.) 250:15-19 (“Q. Okay. So you don’t have any basis to contest that password complexity was enforced on active directory throughout the relevant period? A. For the systems under the control of active directory, I think that’s right.”).

¹²⁰ Ex. 2 (Rattray Rep.) ¶ 175; Ex. 50 (Graff Dep.) 255:21-256:7 (“Q. Okay. So for that part of the process, you’d require the person who was creating the password to manually make it complex; that’s what you’d be depending on? A. In other words, if you want to enforce password complexity, you’re saying you’d have to have the person that created the password follow that guideline? Q. Right. A. Yes, that sounds right. Q. And human compliance is always subject to error? A. I agree with that.”); Zimmerman Decl. ¶ 6.

¹²¹ Ex. 50 (Graff Dep.) 256:17-259:9 (“Q. But this is only one noncomplex password that you were able to find out of the thousands that would have been used at the company? Well, I wasn’t looking for them. ... Q. So you have no evidence that it was a frequent occurrence at SolarWinds to use noncomplex passwords? A. Frequent? I didn’t really address frequency. But—see if I can agree with that. I don’t think I have evidence that shows it was a frequent problem.”).

114. While the security researcher who found the password was concerned that it could be used to distribute malicious software to alter the files SolarWinds made available to customers for download, in fact the password did not have this ability.¹²²

115. There is no evidence that the password was ever discovered by a malicious actor.¹²³

116. The password was promptly changed after SolarWinds received the security researcher's report.¹²⁴

D. Control Deficiencies found in FY 2019 SOX Audit

117. The SEC cites a March 2020 spreadsheet prepared by Danielle Campbell, who ran SolarWinds' Internal Audit program, which indicated that a Fiscal Year 2019 SOX audit found certain "control deficiencies" relating to access controls and passwords.¹²⁵

118. None of the control deficiencies were deemed "significant deficiencies"—which must be reported to management—or "material weaknesses"—which must be reported to investors.¹²⁶

119. Rather, the deficiencies were all merely control deficiencies, which are minor by comparison and not considered to pose any risk to the accuracy of a company's financial statements (which is the focus of a SOX audit).¹²⁷

¹²² Zimmerman Decl. ¶¶ 7-9; Brown Decl. ¶¶ 18-20.

¹²³ Zimmerman Decl. ¶ 10.

¹²⁴ Zimmerman Decl. ¶ 10.

¹²⁵ JS ¶ 188; Ex. 36 (SW-SEC00388330) at -330; Campbell Decl. ¶¶ 3-5.

¹²⁶ Ex. 36 (SW-SEC00388330) at pdf p. 6-7; Campbell Decl. ¶ 5; Ex. 61 (Campbell Inv.) 180:10-16 (confirming that none of the control deficiencies were "significant" nor "material").

¹²⁷ Campbell Decl. ¶¶ 4-5, 9; Ex. 61 (Campbell Inv.) 180:17-181:10 (explaining that a control deficiency is a "lower risk" compared to significant deficiencies and material weaknesses).

120. Ms. Campbell’s spreadsheet specifically explained why none of the control deficiencies found was considered to have a “pervasive” impact.¹²⁸

121. Only two of the deficiencies related to password requirements.¹²⁹

122. Both deficiencies concerned systems on which password complexity requirements were enforced, but not password age and history requirements (*i.e.*, requirements that, after a certain number of days, passwords be changed to a password not previously used by the user).¹³⁰

123. The Security Statement says nothing about password age and history requirements.¹³¹

124. Moreover, both password-related deficiencies were considered minor, because both of the systems at issue could generally only be accessed after logging into SolarWinds’ corporate network, and password age and history requirements *were* enforced on the network login, through Active Directory.¹³²

IV. DOCUMENTS THE SEC RELIES ON AS TO THE SECURE DEVELOPMENT LIFECYCLE REPRESENTATION

A. January 2018 Email about “Feedback” on Secure Software Development

125. The SEC cites an email sent on January 30, 2018, approximately nine months before the Relevant Period, from Steven Colquitt, a Director of Engineering, to engineering managers, stating he had “gotten feedback that we don’t do some of the things that are indicated”

¹²⁸ Ex. 36 (SW-SEC00388330) at pdf p. 6-7, column M; Campbell Decl. ¶ 6; Ex. 61 (Campbell Inv.) 181:11-184:17 (explaining that all control deficiencies were reported to the Audit Committee “whether significant or not” and that Campbell was not aware of “any systemic issue with respect to the level of review and approvals required during the change management process”).

¹²⁹ Campbell Decl. ¶ 7; Ex. 36 (SW-SEC00388330) at pdf p. 6, lines 7 & 25.

¹³⁰ Campbell Decl. ¶ 7; Ex. 36 (SW-SEC00388330) at pdf p. 6, lines 7 & 25.

¹³¹ Ex. 1 (Security Statement) at 3.

¹³² Ex. 36 (SW-SEC00388330) (noting that both were considered “Low Risk” because “[i]nstances in which users are logging in outside of” the Active Directory were “not nearly as common”); Campbell Decl. ¶¶ 7-9.

in the Security Statement's section on secure software development. Mr. Colquitt continued in the email:

I want to make sure that you all have an answer to this. The simple response is: There is improvement needed to be able to meet the security expectation of a Secure Development Lifecycle. We will be working with teams throughout 2018 to begin incorporating the SDL into their development lifecycle. This begins with general SDL training for all Engineering along with several SDL pilots with specific teams in Q1. We'll continue to pragmatically roll out the SDL to additional teams each quarter."¹³³

126. Around this time, Mr. Colquitt was working on a project to formalize and improve documentation of SolarWinds' secure development practices, as part of a company-wide project to prepare for new regulatory requirements coming into effect in May 2018.¹³⁴

127. Mr. Colquitt knew from years of working as a software engineer at SolarWinds that SolarWinds' development teams already conducted security testing as part of their software development practices. He was seeking to overlay a new framework on these activities to make them more consistent across the organization and to improve documentation around them.¹³⁵

¹³³ JS ¶ 190; Ex. 11 (SW-SEC00238141) at -141; Colquitt Decl. ¶ 2.

¹³⁴ Colquitt Decl. ¶¶ 3-5; Ex. 60 (Colquitt Dep.) 17:7-16 (noting Company's "preparing to be ready for GDPR compliance in May of 2018"), 58:19-25 ("The SDL was an overlay on top of that that exposed and gave visibility into these activities at a much higher level and centralized and formalized that documentation.").

¹³⁵ Colquitt Decl. ¶¶ 4, 13; Ex. 60 (Colquitt Dep.) 58:19-25 ("The SDL was an overlay on top of that that exposed and gave visibility into those activities at a much higher level and centralized and formalized that documentation"); 98:8-18 ("The SDL will help consolidate these activities, formalize and standardize these activities"); Ex. 46 (Brown Dep.) 127:25-128:4 ("We ... had at that period of time acquired a number of different solutions and a number of different companies, and those companies came in with their own practices. So standardizing knowledge across the organization was part of [the] goal [of Steven's project].").

128. As part of this effort, Mr. Colquitt developed new internal policy documentation describing the secure development processes that all teams should follow, which he labeled the Company's "Secure Development Lifecycle," or "SDL."¹³⁶

129. Mr. Colquitt also developed new documentation requirements as part of the SDL, including a requirement that development teams prepare a Final Security Review before launching a software release to document the security-related activities that went into the development of the release.¹³⁷

130. Mr. Colquitt also developed an internal training for all software engineers at the company to familiarize them with the SDL framework. This training was designed for *all* engineers—not just those with a security-related role.¹³⁸ The purpose of the training was to increase visibility across the engineering organization into the Company's secure development practices and activities and to make sure everyone understood the importance of these activities.¹³⁹

131. In late January, Mr. Colquitt was preparing to deliver this training. In anticipation of that, he thought it would be useful for all software development team members to be familiar

¹³⁶ Colquitt Decl. ¶ 5; Ex. 60 (Colquitt Dep.) 44:25-45:3 ("I was introducing a new process to overlay our security activities that we were labeling Secure Development Lifecycle, capital S, capital D, capital L. That was the title.").

¹³⁷ Colquitt Decl. ¶ 5; Ex. 60 (Colquitt Dep.) 31:25-32:6 (noting that goal of final security review was that "rather than having each team independently do their reviews and sign off, it was bringing them all together for a complete view of the posture, just to improve the visibility of what the teams have been doing from their testing and design").

¹³⁸ Colquitt Decl. ¶ 6; Ex. 60 (Colquitt Dep.) 192:2-7 (noting that training included "[a]ll engineers, whether they were involved in security activities or not").

¹³⁹ Colquitt Decl. ¶ 6; Ex. 60 (Colquitt Dep.) 195:9-19 ("Training broadly across the engineering teams introduced a formality and a consistency in our approach that some of those engineers might not have been familiar with prior, so this training brought that level of awareness to each of those individuals"); Ex. 46 (Brown Dep.) 127:11-128:8 (explaining that some engineers were uninvolved in security aspects of development and unaware of security requirements, "[s]o Steven's training was to level set across [the] organization" by "train[ing] every developer on development practices [to] make them aware of additional resources for secure development").

with what SolarWinds publicly said about secure software development in the Company's Security Statement, which had only recently been added to the Company's website.¹⁴⁰

132. On January 25, 2018, Mr. Colquitt sent the "Software Development Lifecycle" section of the Security Statement to all engineering managers, asking them to share it with their teams.¹⁴¹

133. Five days later, on January 30, 2018, Mr. Colquitt got an email from one of these engineering managers, stating "[t]his is great progress in formalizing our security process," leading to a discussion in which Mr. Colquitt explained he would be beginning his general SDL trainings soon. Mr. Vrbecky wrote back:

I think that would be great. It came back from teams as a feedback that we actually don't do things and actions that are in the statement. I'd say more accurate would be that teams are not fully aware about the scope of what we do and also what are we going to do by the end of Q1. For these kind of questions coming from team, I'd like managers to have canned answer.¹⁴²

134. Mr. Colquitt was not surprised that some engineers may not have known about the security testing that was already part of SolarWinds' software development processes.¹⁴³ He had asked engineering managers to share the excerpt from the Security Statement with *all* software engineers, not just those involved in the security aspects of development, so some of the recipients would not have been familiar with those aspects.¹⁴⁴ That is what Mr. Colquitt understood Mr.

¹⁴⁰ Colquitt Decl. ¶ 7; Ex. 11 (SW-SEC00238141) at -141.

¹⁴¹ Ex. 11 (SW-SEC00238141) at -141; Colquitt Decl. ¶ 7; Ex. 60 (Colquitt Dep.) 94:11-95:7 (explaining that the inclusion of the SDL portion of the Security Statement was motivated by "awareness"), 198:9-12.

¹⁴² Ex. 12 (SW-SEC-SDNY_00055079) at -079; Colquitt Decl. ¶ 8.

¹⁴³ Colquitt Decl. ¶ 9; Ex. 60 (Colquitt Dep.) 200:19-201:7 (acknowledging that "there were engineers on teams who probably weren't involved in aspects of things like pen testing, vulnerability testing, who didn't have direct knowledge that those activities were happening").

¹⁴⁴ Colquitt Decl. ¶ 9; Ex. 60 (Colquitt Dep.) 198:9-23.

Vrbecky to mean by saying: “I’d say more accurate would be that teams are not fully aware about the scope of what we do.”¹⁴⁵

135. Mr. Colquitt responded to Mr. Vrbecky’s email—which had asked for a “canned answer” that engineering managers could provide in response to any similar feedback—by sending another email to all engineering managers a few hours later, with a response they could provide, which is the email cited by the SEC.¹⁴⁶

136. In stating there was “improvement needed,” Mr. Colquitt’s intent was to encourage engineers to attend the trainings he was planning and to generate interest in the SDL framework that he had developed.¹⁴⁷

137. Mr. Colquitt also believed there was improvement the Company needed to make to its software development practices—including around documentation, and raising security awareness across the engineering organization.¹⁴⁸

138. Mr. Colquitt did not mean to suggest that SolarWinds was not doing the types of security testing described in the Security Statement.¹⁴⁹

¹⁴⁵ Colquitt Decl. ¶ 9; Ex. 60 (Colquitt Dep.) 200:19-201:7.

¹⁴⁶ Ex. 11 (SW-SEC00238141) at -141; Colquitt Decl. ¶ 10; Ex. 60 (Colquitt Dep.) 102:17-24.

¹⁴⁷ Colquitt Decl. ¶¶ 11-13; Ex. 60 (Colquitt Dep.) 98:15-18, 101:4-19, 201:14-202:5 (“Q. And what type of improvements, again, was your SDL project focused on making? A. Again, mainly it brought awareness; two, it formalized the outputs, formalized documentation; and, third, it introduced some additional process that would facilitate bringing that documentation together”).

¹⁴⁸ Ex. 60 (Colquitt Dep.) 98:15-18, 201:24-202:5; Colquitt Decl. ¶ 11.

¹⁴⁹ Ex. 60 (Colquitt Dep.) 80:21-24 (“If you’re asking me if we were applying the activities that supported what is listed in the security statement, the answer is yes”), 98:2-18; Colquitt Decl. ¶ 12.

B. February 2019 Slide about Goals for MSP Engineering

139. The SEC cites a slide from a deck sent in a February 13, 2019 email to all engineering staff within SolarWinds’ MSP (Managed Service Provider) business line, which lists several goals for the group to “Grow Together.”¹⁵⁰

140. The cited slide lists as among the “Goals” for FY 2019: “Improve security both in our products and our positioning,” “Audit MSP Engineering training level and adoption of SDL (Secure Development Lifecycle),” and “Drive down the number of incidents introduced by MSP Engineering.”¹⁵¹

141. These statements simply reflected that SolarWinds wanted to continue improving its secure development practices and standardizing those practices across its product lines. In particular, the reference to “adoption of SDL” was a reference to Stephen Colquitt’s project to standardize and formalize SolarWinds’ already existing practices.¹⁵²

142. None of the stated goals were meant to suggest that MSP engineers pervasively failed to do security testing as part of their software development.¹⁵³

¹⁵⁰ JS ¶ 193; Ex. 21 (SW-SEC-SDNY_00000004) at pdf p. 5; Ex. 59 (Kim Dep.) 170:9-172:24.

¹⁵¹ Ex. 59 (Kim Dep.) 176:16-185:24; Ex. 21 (SW-SEC-SDNY_00000004) at pdf p. 7.

¹⁵² Ex. 59 (Kim Dep.) 176:16-177:19 (“[O]ne of the things that I did want to make sure is that we continue improvement around the security stance and standardization across products. So here in terms of SDL, it’s the project that I had Steven Colquitt and Tim Brown launch to see if we can better standardize and improve product security.”); Ex. 50 (Graff Dep.) 184:3-7 (agreeing “that cybersecurity is a process of continuous improvement.”).

¹⁵³ Ex. 59 (Kim Dep.) 178:22-179:18 (“If I had to interpret it, he probably means the new SDL kind of initiative that Tim and Steven had launched [regarding documentation], and as part of their finding[] some additional training that they’re putting in place to make sure that MSP engineering teams are, you know, getting trained on ... the findings from that initiative.”); Ex. 59 (Kim Dep.) 117:9-118:11 (testifying that the “software development lifecycle” section of the Security Statement “was true at the time I was at SolarWinds” because “as stated here, things like vulnerability testing, regression testing, penetration testing and product security assessments were conducted on the products as part of the SDLC”).

C. Documents about Penetration Testing

1. Budget Item for External Penetration Testing in November 2018 Slide Deck

143. The SEC cites a November 2018 slide deck entitled “SolarWinds KBT Offsite DOIT and R&D,” which included a slide titled, “FY18 Initiatives.” A row of a chart on the slide contains an entry for “PEN Testing” with the note: “Unfunded in FY18. Plan to PEN test 8-10 products in 2019.”¹⁵⁴

144. This was a reference to a specific budget item for *external* penetration testing—*i.e.*, penetration testing conducted by a third-party vendor, rather than penetration testing conducted internally by SolarWinds software engineers.¹⁵⁵

145. External penetration testing required separate budget in order to engage the third-party vendor, unlike internal penetration testing that was conducted with personnel already on the SolarWinds payroll.¹⁵⁶

146. External penetration testing supplemented internal penetration testing done by SolarWinds.¹⁵⁷

147. The fact that a particular budget request for external penetration testing went unfunded for FY2018 does not imply that no internal penetration testing was done in FY2018.¹⁵⁸

¹⁵⁴ JS ¶ 192; Ex. 20 (SW-SEC00298924) at -934.

¹⁵⁵ Brown Decl. ¶¶ 13-14.

¹⁵⁶ Brown Decl. ¶ 14.

¹⁵⁷ Brown Decl. ¶ 14; Ex. 46 (Brown Dep.) 134:10-22 (“[P]enetration testing was definitely done from an internal perspective and in some cases an external perspective”); Ex. 23 (SW-SEC00016539) at -546 (excerpts from slide deck showing schedule for “External (3rd Party) Pen Testing Program” and “Internal Pen Testing Program”).

¹⁵⁸ Brown Decl. ¶ 14; JS ¶ 148; Ex. 60 (Colquitt Dep.) 48:1-23 (“We were doing ... penetration testing”), 119:13-120:20 (testifying his teams did penetration testing); Ex. 59 (Kim Dep.) 116:14-118:11 (“[P]enetration testing ... w[as] conducted on the products as part of the SDLC.”); 134:14-135:10; Ex. 45

148. The fact that a particular budget request for external penetration testing went unfunded for FY 2018 does not even imply that no external penetration testing was done in FY2018, as external penetration testing could have been funded through other means.¹⁵⁹

149. In fact, external penetration testing of certain products was completed in FY2018, including the Company's MSP and Cloud products.¹⁶⁰

2. July 2020 Slide about Testing in Final Security Reviews

150. The SEC cites a slide titled "ITOM Core Highlights and Asks" from a July 2020 deck prepared by Tim Brown, which states: "Inconsistent internal security testing as part of product final security reviews don't always include web application testing before release" and "[c]ustomers continue to actively engage 3rd party penetration testers as part of their compliance efforts[.]"¹⁶¹

151. The statement "Inconsistent internal security testing as part of product final security reviews don't always include web application testing before release" simply indicates that Final Security Reviews being prepared by software development teams did not "always" include web application testing results, which could mean either that the testing was not being done in those instances or that the results were not being included in the Final Security Reviews.¹⁶²

(Bliss Dep.) 134:9-135:2 (testifying "Software Development Life Cycle" part of the Security Statement "was accurate"); Colquitt Decl. ¶¶ 4, 12-13.

¹⁵⁹ Brown Decl. ¶ 1.

¹⁶⁰ Brown Decl. ¶ 1; Ex. 33 (SW-SEC00295588) (excerpts from slide deck titled "Summary of PEN Test results for MSP and Cloud performed Q2 2018" showing products covered by the testing; details of test results excluded).

¹⁶¹ JS ¶ 200.

¹⁶² Brown Decl. ¶¶ 15-16; Ex. 45 (Bliss Dep.) 264:4-18 ("[M]y interpretation of this is this is an improvement on the overall program that you're looking at.").

152. The statement does not indicate there was any pervasive failure to do web application testing.¹⁶³

153. Under the statement there are references to “Checkmarx” and “Whitesource”—two testing products used by SolarWinds—indicating that these tools were available for engineers to use for web application testing.¹⁶⁴

154. Hundreds of records generated from the use of these tools during the Relevant Period were produced in discovery.¹⁶⁵

155. The statement that “[c]ustomers continue to actively engage 3rd party penetration testers as part of their compliance efforts” simply indicates that some customers were conducting independent penetration testing of SolarWinds’ products as part of their own compliance programs.¹⁶⁶

156. The statement does not imply that SolarWinds was not conducting penetration testing.¹⁶⁷

¹⁶³ Brown Decl. ¶¶ 15-16.

¹⁶⁴ Ex. 2 (Rattray Rep.) ¶ 95; Ex. 45 (Bliss Dep.) 264:19-265:6 (CheckMarx and Whitesource are “tool[s] in the development life cycle.”).

¹⁶⁵ Ex. 2 (Rattray Rep.) ¶¶ 95-96 (referencing and citing these records).

¹⁶⁶ Brown Decl. ¶¶ 16-17; Ex. 45 (Bliss Dep.) 265:19-266:5 (“My general experience with these customer inquiries is there are a number of penetration tools that were out there and we used some and they were good. Customers sometimes use a different tool and would not necessarily rely on what the company had done with their tool.”).

¹⁶⁷ Brown Decl. ¶ 1; *see also* Ex. 45 (Bliss Dep.) 134:9-135:2; 265:19-21 (Q: “Was this a statement that SolarWinds’s penetration testing was inadequate? A: No.”); Ex. 60 (Colquitt Dep.) 48:1-23, 119:13-120:20; Ex. 59 (Kim Dep.) 116:14-118:11, 134:14-135:10.

D. Documents about Threat Modeling

1. May 2018 Email about Tool for Threat Modeling

157. The SEC cites a May 21, 2018 email from Rani Johnson to Tim Brown and Steven Colquitt and email with a subject line “Please confirm (particularly the threat modeling).” The body of the email included a list of tools used for “security capabilities,” including PEN testing, vulnerability assessment/scanning, network monitoring, access control, and others.¹⁶⁸

158. Mr. Colquitt replied that, “I don’t see a line item about threat modeling ... but since you mentioned it. [Threat modeling] is a process. It’s part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity. So I am not sure what you are looking for in terms of confirmation.”¹⁶⁹

159. In saying “threat modeling” was “part of the SDL,” Mr. Colquitt was saying it was part of the internal policy documentation he developed describing the secure development processes that all teams should follow.¹⁷⁰

160. The Security Statement itself does not mention anything about “threat modeling.”¹⁷¹

¹⁶⁸ JS ¶ 191; Ex. 17 (SW-SEC00237608) at -608-09; Ex. 60 (Colquitt Dep.) 143:2-9.

¹⁶⁹ Ex. 17 (SW-SEC00237608) at -608; Ex. 60 (Colquitt Dep.) 138:17-20.

¹⁷⁰ Ex. 60 (Colquitt Dep.) 139:1-12 (Q: “What did you mean that threat modeling is part of the SDL? A: ... Currently the artifacts that were coming from the threat modeling that we were doing were not well documented And part of my project was to improve the artifacts that were coming from those activities in a more formal, formal manner.”).

¹⁷¹ Ex. 1 (Security Statement) at 3; Ex. 60 (Colquitt Dep.) 139:3–24 (“[Threat modeling] was an additional thing that’s not part of our security statement.”).

161. Mr. Colquitt understood the term “threat modeling” to be a broad term that can encompass many different types of activities designed to anticipate and address security risks in software functionality.¹⁷²

162. In Mr. Colquitt’s understanding, “[t]hreat modeling can be done verbally, it can be done on a piece of paper, it can be done on a whiteboard or you can use a formal tool to produce that documentation. There are multiple ways to do this exercise.”¹⁷³

163. In saying that “we are just barely beginning to understand how teams are going to be doing this activity,” Mr. Colquitt was not “talking about doing the threat modeling itself,” which “was already happening” at SolarWinds.¹⁷⁴

164. Mr. Colquitt was talking about how teams were going to be *documenting* the activity of threat modeling.¹⁷⁵

¹⁷² Ex. 60 (Colquitt Dep.) 65:14-23 (“This exchange we just had where I explained that when I assess a particular requirement, I identify a risk and I mitigate that risk, that is threat modeling.”), 144:23-145:8, 165:6-20 (stating that threat modeling is “an inherent aspect of implementing a mitigation to a security risk”: “As an engineer when you are implementing a piece of functionality, you will assess the user or data interaction in that piece of functionality and you will assess whether there’s a risk there. And if there is, you will put in a mitigation.”), 206:5-207:2 (“[Threat modeling is] when you assess the risk that there might be an opportunity for someone to sort of get around the security that you’ve implemented in your product.”).

¹⁷³ Ex. 60 (Colquitt Dep.) 144:23-145:8; *see also* Ex. 50 (Graff Dep.) 9:16-20 (“There are different levels of formalities you can use when you do cybersecurity assessments.”); Ex. 2 (Rattray Rep.) ¶¶ 207-208 (“‘Threat modeling’ is a loose term that can encompass virtually any effort to anticipate and address potential security threats as part of the software design process”).

¹⁷⁴ Ex. 60 (Colquitt Dep.) 142:16-19 (“Q: Okay. So you don’t think you were talking about doing the threat modeling itself here? A: Threat modeling, no. It was already happening.”).

¹⁷⁵ Ex. 60 (Colquitt Dep.) 142:1-10 (“I wanted to improve the process. I was trying to determine what options we had in terms of producing that documentation and tracking that documentation that I had not yet settled on.”).

165. As part of his standardization project, Mr. Colquitt was still looking to “determine what options we had in terms of producing [] documentation” of threat modeling and “tracking that documentation.”¹⁷⁶

166. In particular, Mr. Colquitt was responding to an email sent from Ms. Johnson, who was collecting information about what sort of tooling was used for different security activities, and he was conveying that threat modeling was a “process” that would not necessarily be accomplished with a “formal tool.”¹⁷⁷

2. July 2019 MSP Products Evaluations

167. The SEC cites a document dated July 2019 titled, “MSP Products Evaluation.”¹⁷⁸

168. The report covers three MSP products—RMM, NCentral and Backup.¹⁷⁹

169. A line in the report states, “No threat modelling nor analysis is performed as part of any process (except MSP Backup Engineering).”¹⁸⁰

170. The SEC cites a similar evaluation for the MSP product MailAssure, dated December 2019, which contains a similar line.¹⁸¹

171. The SEC did not depose the authors of these documents in order to understand the meaning of this statement or what they meant exactly by “threat modeling.”

¹⁷⁶ Ex. 60 (Colquitt Dep.) 142:1-10.

¹⁷⁷ Ex. 60 (Colquitt Dep.) 144:10-145:8 (explaining that “I was implying that I wanted to improve the process,” which would not necessarily involve a “formal tool”).

¹⁷⁸ JS ¶ 195.

¹⁷⁹ JS ¶ 195.

¹⁸⁰ JS ¶ 195.

¹⁸¹ JS ¶ 196.

172. SolarWinds’ development teams within the MSP organization may not have done formalized threat modeling at the time these documents were prepared in July and December 2019, but they did analyze products for security risks and vulnerabilities.¹⁸²

173. Final Security Reviews for releases of the RMM, NCentral and Backup products developed during the Relevant Period contain sections concerning “Vulnerabilities Addressed in Current Release,” which in turn contain records of engineers identifying “risks” during the development process and proposing or implementing a “fix” or “mitigation” for each. These include records of such analysis being conducted around and before July 2019.¹⁸³

E. June 2020 Email about Orion Improvement Program

174. The SEC cites an email exchange from June 2020 with the subject line “SDL and Orion Improvement Program,” in which a SolarWinds engineer stated in part “Do we have SDL process enforced for Orion Improvement Program server? If SDL is not enforced for OIP, we should do it ASAP and consider additional actions to make sure that OIP is very well protected.” Another engineer responded, “I don’t believe we cover OIP today with the SDL, but we should.” The SEC has argued that the fact that the Company’s “SDL”—*i.e.*, its secure development process—did not cover the Orion Improvement Program (OIP) at the time contradicts the Security Statement.¹⁸⁴

¹⁸² Ex. 60 (Colquitt Dep.) 170:22-171:5 (“I cannot speak to any of the MSP products or MSP engineering. I can speak to generally it’s impossible to deliver security controls in a product without having done threat analysis.”), 171:13-23 (“I don’t understand what criteria they’re using here to make that assessment. They may have been thinking of more of a formal process that they would like to achieve.”), 206:15-207:2.

¹⁸³ Ex. 2 (Rattray Rep.) ¶¶ 212-13.

¹⁸⁴ JS ¶ 199; AC ¶¶ 131–35.

175. The Security Statement’s section on software development discusses what SolarWinds does “to increase the resiliency and trustworthiness of *our products*.”¹⁸⁵

176. OIP was not a SolarWinds product or a component of a SolarWinds product.¹⁸⁶

177. OIP was an internal business application that SolarWinds used to collect Orion usage information from customers who agreed to provide it, in order to help advise customers on how to improve their deployment of the software.¹⁸⁷

178. The OIP application ran on SolarWinds’ own server, not on customer infrastructure.¹⁸⁸

179. The suggestion in the cited email chain to “cover OIP ... with the SDL” was made in the context of SolarWinds’ investigation of an incident reported by the Department of Justice’s

¹⁸⁵ Ex. 1 (Security Statement) at 3; Ex. 50 (Graff Dep.) 286:7-15 (Q: “Would you agree that the term ‘products’ typically refers to the things that a company sells to its customers? A: Yes.”); Ex. 2 (Rattray Rep.) ¶¶ 197-98 (“SolarWinds’ software development lifecycle [in] the Security Statement refers to ‘our products’—a term that [Mr. Graff] himself uses in his report to refer to software sold to SolarWinds’ customers.”).

¹⁸⁶ Ex. 48 (Brown Inv. Vol. II) 380:12-381:4 (“[T]he OIP server that’s talked about is our internally-hosted server That’s what OIP is. ... [I]t’s something inside of our environment. It’s not a product we sell, it’s not a solution that is, you know, offered to customers or anything like that.”), 394:20-395:12; Ex. 50 (Graff Dep.) 288:22-25 (Q: “[W]ould you agree that the OIP software application was not a product that SolarWinds sold to customers? A: Yes, that’s my understanding.”); 290:7-12 (“Well, the OIP application was not a product, I agree with that.”); Ex. 2 (Rattray Rep.) ¶ 199 (“OIP was not software that SolarWinds *customers* used; it resided on SolarWinds own network and was used *by SolarWinds*.”).

¹⁸⁷ Ex. 48 (Brown Inv. Vol. II) 394:20-395:7 (“So these are called Bizapps, business applications. One of those business applications is OIP. That business application was built internally for the specific purpose of collecting information and helping customers with their deployment.”); Ex. 53 (Johnson Inv. Vol. II) 207:13-16 (“Q. And what is your understanding of what the Orion Improvement Program is? A. It was a server that collected information related to customers’ usage of Orion.”).

¹⁸⁸ Ex. 48 (Brown Inv. Vol. II) 380:12-381:4 (“The OIP server sits inside of our environment and it takes information from clients to essentially improve their product. But it’s a separate application, not something that’s commercial. It’s something that’s inside of our environment to talk to.”); Ex. 49 (Cline Dep.) 15:6-13 (explaining that BizApps are SolarWinds “business applications” and “very much focused on the application side that the business runs off of”); Ex. 2 (Rattray Rep.) ¶¶ 199-200.

U.S. Trustee Program (“USTP”)—the same incident that is discussed in the SEC’s Amended Complaint involving “U.S. Government Agency A.”¹⁸⁹

180. In initially responding to the report, SolarWinds’ InfoSec team was concerned that an attacker might be trying to *attack SolarWinds* through the OIP server.¹⁹⁰

181. In that context, the Infosec team sought to harden the OIP server against attack by applying the same sort of testing to OIP that the Company would do as part of its software development lifecycle for customer products. The decision to do so was not made because OIP was such a product or because the testing was supposed to have been done earlier, but because this particular incident raised a concern that OIP was potentially being targeted as part of an attack on SolarWinds.¹⁹¹

¹⁸⁹ AC ¶¶ 268-278; Ex. 2 (Ratray Rep.) ¶ 202.

¹⁹⁰ Ex. 48 (Brown Inv. Vol. II) 381:18-382:9 (“So our theory with this is that ... either the box [i.e., server] that [USTP] installed [Orion] on was a dirty box and had [malicious code on it], or that, you know, the box itself had been compromised without us and that that [malicious code] was attacking SolarWinds with that OIP layer. So that’s why you’ll see a lot of hardening on OIP. ... We essentially brought in everybody to look at this traffic and this incident.”); Ex. 2 (Ratray Rep.) ¶ 202.

¹⁹¹ Ex. 48 (Brown Inv. Vol. II) 388:10-21 (“[W]hen you build a product for internal use, not a product but a service that you’re going to use internally[,] that doesn’t necessarily follow the same processes that when we build the products from the outside. But we implemented a number of those processes around the OIP server and investigated the server itself and then, you know, made some changes to the OIP server to make sure that—you know, that it was hardened against attacks. Although we couldn’t tell what the attack was from the data we had, [we] essentially looked everywhere we could and put as many safeguards in place on the OIP server so it wouldn’t affect us.”); Ex. 2 (Ratray Rep.) ¶¶ 202-04.

Dated: April 25, 2025

Respectfully submitted,



Serrin Turner

Matthew Valenti

Nicolas Luongo

LATHAM & WATKINS LLP

1271 Avenue of the Americas

New York, NY 10020

Telephone: (212) 906-1200

Facsimile: (212) 751-4864

serrin.turner@lw.com

matthew.valenti@lw.com

nicolas.luongo@lw.com

Sean M. Berkowitz (*pro hac vice*)

LATHAM & WATKINS LLP

330 N. Wabash, Suite 2800

Chicago, IL 60611

Telephone: (312) 876-7700


Facsimile: (617) 993-9767

sean.berkowitz@lw.com

*Counsel for Defendants SolarWinds Corp. and Timothy
G. Brown*

CERTIFICATE OF SERVICE

I hereby certify that on April 25, 2025, I electronically filed the foregoing document with the Court via CM/ECF, which will automatically send notice and a copy of same to counsel of record via email.


Serrin Turner